CLAIMS

What is claimed is:

1. A method for performing path-level access control evaluation for a structured document in a collection, wherein the structured document comprises a plurality of nodes and each of the nodes is described by a path, the method comprising the steps of:

a) providing a cache for temporarily storing a cache entry for a path associated with a node of the plurality of nodes;

b) receiving a query, wherein the query comprises a request to access the node;

c) checking the cache entry for the path associated with the node; and

d) determining whether to grant access to the node based on the cache entry.

2. The method of claim 1, wherein the cache entry is one of a grant, deny, unknown and data-dependent statement.

3. The method of claim 2, wherein determining step (d) further comprising:

(d1) granting access to the node if the cache entry is a grant statement.

4. The method of claim 2, wherein determining step (d) further comprising:

(d1) denying access to the node if the cache entry is a deny statement.

5. The method of claim 2, wherein determining step (d) further comprising:

(d1) evaluating an access control policy for the structured document affecting the path if the cache entry is an unknown statement;

(d2) granting access if a result of the evaluation in step (d1) grants access; and

(d3) denying access if the result of the evaluation in step (d1) denies access.

6. The method of claim 5 further comprising:

(e) determining whether the access control policy affecting the path is data-dependent;

(f) changing the cache entry from the unknown statement to a grant or a deny statement based on the evaluation in step (d1) if the access control policy affecting the path is not data-dependent; and

(g) changing the cache entry from the unknown statement to a data-dependent statement if the access control policy affecting the path is data-dependent.

7. The method of claim 2, wherein determining step (d) further comprising:

(d1) evaluating an access control policy for the structured document affecting the path if the cache entry is a data-dependent statement;

(d2) granting access if a result of the evaluation in step (d1) grants access; and

(d3) denying access if the result of the evaluation in step (d1) denies access.

8. The method of claim 1, further comprising:

(e) repeating checking and determining steps (c) and (d) for a next node.

9. The method of claim 5, wherein evaluating step (d1) further comprises:

(d1i) evaluating a value expression for the path associated with the node,

wherein the value expression is an executable statement based on the access control policy affecting the path and indicates who has access to the node.

10. The method of claim 9, wherein checking and determining steps (c) and (d) are performed during a run time.

11. A computer readable medium containing programming instructions for performing path-level access control evaluation for a structured document in a collection, wherein the structured document comprises a plurality of nodes and each of the nodes is described by a path, the programming instructions for:

a) providing a cache for temporarily storing a cache entry for a path associated with a node of the plurality of nodes;

b) receiving a query, wherein the query comprises a request to access the node;

c) checking the cache entry for the path associated with the node; and

d) determining whether to grant access to the node based on the cache entry.

12. The computer readable medium of claim 11, wherein the cache entry is one of a grant, deny, unknown and data-dependent statement.

13. The computer readable medium of claim 12, wherein determining instruction (d) further comprising:

(d1) granting access to the node if the cache entry is a grant statement.

14. The computer readable medium of claim 12, wherein determining instruction (d) further comprising:

(d1) denying access to the node if the cache entry is a deny statement.

15. The computer readable medium of claim 12, wherein determining instruction (d) further comprising:

(d1) evaluating an access control policy for the structured document affecting the path if the cache entry is an unknown statement;

(d2) granting access if a result of the evaluation in instruction (d1) grants access; and

(d3) denying access if the result of the evaluation in instruction (d1) denies access.

16. The computer readable medium of claim 15 further comprising:

(e) determining whether the access control policy affecting the path is data-dependent;

(f) changing the cache entry from the unknown statement to a grant or a deny statement based on the evaluation in instruction (d1) if the access control policy affecting the path is not data-dependent; and

(g) changing the cache entry from the unknown statement to a data-dependent statement if the access control policy affecting the path is data-dependent.

17. The computer readable medium of claim 12, wherein determining instruction (d)

further comprising:

(d1) evaluating an access control policy for the structured document affecting the path if the cache entry is a data-dependent statement;

(d2) granting access if a result of the evaluation in instruction (d1) grants access; and

(d3) denying access if the result of the evaluation in instruction (d1) denies access.

18. The computer readable medium of claim 11, further comprising:

(e) repeating checking and determining instructions (c) and (d) for a next node.

19. The computer readable medium of claim 15, wherein evaluating instruction (d1) further comprises:

(d1i) evaluating a value expression for the path associated with the node, wherein the value expression is an executable statement based on the access control policy affecting the path and indicates who has access to the node.

20. The computer readable medium of claim 19, wherein checking and determining instructions (c) and (d) are performed during a run time.

21. A method for performing path-level access control evaluation for a structured document in a collection, wherein the structured document comprises a plurality of nodes and each of the nodes is described by a path, the method comprising the steps of:

a) providing a cache for temporarily storing a cache entry for a path associated with a node of the plurality of nodes, wherein the cache entry is one of a grant, deny, unknown and data-dependent statement;

b) receiving a query, wherein the query comprises a request to access the node;

c) checking the cache entry for the path associated with the node;

d) granting access to the node if the cache entry is a grant statement;

e) denying access to the node if the cache entry is a deny statement; and

f) determining access control if the cache entry is an unknown or data-dependent statement.

22. The method of claim 21, wherein the determining step (f) further comprising:

f1) evaluating a value expression for the path associated with the node, wherein the value expression is an executable statement based on an access control policy affecting the path and indicates who has access to the node;

f2) granting or denying access to the node based on a result of the evaluation in step (f1);

f3) changing the cache entry to a grant or deny statement based on the result of the evaluation in step (f1) if the access control policy affecting the path is not data-dependent; and

f4) changing the cache entry to a data-dependent statement if the access control policy affecting the path is data-dependent.

23. The method of claim 22 further comprising:

g) repeating steps (c) through (f) for a next node.

24. A computer readable medium containing programming instructions for performing path-level access control evaluation for a structured document in a collection, wherein the structured document comprises a plurality of nodes and each of the nodes is described by a path, the programming instructions for:

a) providing a cache for temporarily storing a cache entry for a path associated with a node of the plurality of nodes, wherein the cache entry is one of a grant, deny, unknown and data-dependent statement;

b) receiving a query, wherein the query comprises a request to access the node;

c) checking the cache entry for the path associated with the node;

d) granting access to the node if the cache entry is a grant statement;

e) denying access to the node if the cache entry is a deny statement; and

f) determining access control if the cache entry is an unknown or data-dependent statement.

25. The computer readable medium of claim 24, wherein the determining instruction (f) further comprising:

f1) evaluating a value expression for the path associated with the node, wherein the value expression is an executable statement based on the access control policy affecting the path and indicates who has access to the node;

f2) granting or denying access to the node based on a result of the evaluation in instruction (f1);

f3) changing the cache entry to a grant or deny statement based on the result of the evaluation in instruction (f1) if the access control policy affecting the path is not data-dependent; and

f4) changing the cache entry to a data-dependent statement if the access control policy affecting the path is data-dependent.

26. The computer readable medium of claim 25 further comprising:

g) repeating instructions (c) through (f) for a next node.

27. A system for performing path-level access control evaluation for a structured document in a collection, wherein the structured document comprises a plurality of nodes and each of the nodes is described by a path, comprising:

a database management system in a computer system for receiving a query, wherein the query comprises a request to access a node of the plurality of nodes; and

a cache in the computer system coupled to the database management system for temporarily storing a cache entry for a path associated with the node;

wherein the database management system is configured to check the cache entry for the path associated with the node and to determine whether to grant or deny access to the node based on the cache entry.

28. The system of claim 27, wherein the cache entry is one of a grant, deny, unknown and data-dependent statement.

29. The system of claim 28 further comprising:

an Access Control mechanism coupled to the database management system for determining access control to the node if the cache entry is an unknown or data-dependent statement.

30. The system of claim 29, wherein the Access Control mechanism is configured to generate for the path associated with the node a corresponding value expression based on an access control policy for the structured document affecting the path, wherein the database management system evaluates the corresponding value expression to determine whether to grant access to the node.

31. The system of claim 30 wherein the database management system is configured to change the cache entry from an unknown statement to a grant or deny statement based on a result of the evaluation of the value expression if the value expression for the path is not data-dependent and to change the cache entry from an unknown statement to a data-dependent statement if the value expression for the path is data-dependent.